PCT

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(54) Title: METHOD AND SYSTEM FOR TRACKING COMPUTER SYSTEM USAGE THROUGH A REMOTE ACCESS SECURITY DEVICE
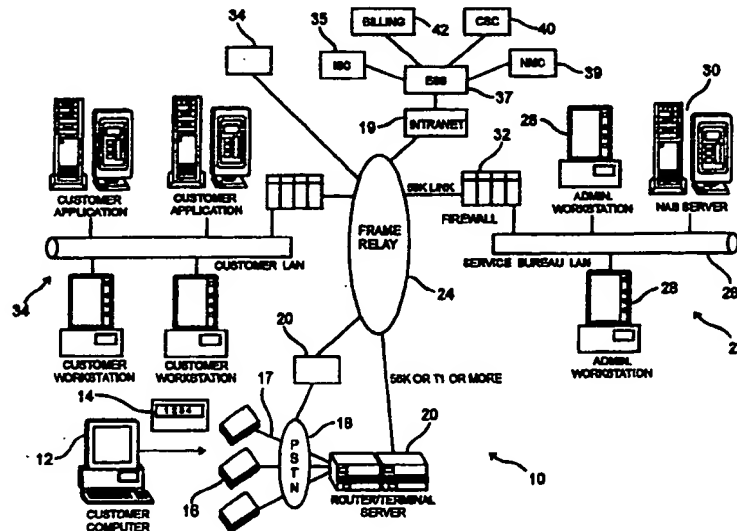
(57) Abstract

A system and method for monitoring remote computer access and associated costs is provided. The system (10) includes a remotely located communication server (20) in communication with multiple host computer networks (34) and in communication with a network access server (30). First and second memory devices contain a list of authorized users for the host computer networks (34) and a user log for user by a billing computer (42) to generate bills. The method includes the steps of creating starting and ending time stamps (step 54) for each authorized user accessing a respective one of the multiple host computer networks (34) and creating a user log to generate bills (step 62) and monitor host computer network usage.

METHOD AND SYSTEM FOR TRACKING COMPUTER SYSTEM USAGE THROUGH A REMOTE ACCESS SECURITY DEVICE

5

BACKGROUND OF THE INVENTION

10

The present invention relates to a system and method for monitoring access to each of a plurality of unrelated host computer networks. More particularly, the present invention relates to a system and method of tracking computer usage, and costs associated with the computer usage, by authorized users of different computer networks.

15

Many organizations, both in government and in private industry, rely on access to centralized computer facilities. Use of remote access capabilities to centralized computer facilities is generally desirable in order to facilitate use of computer resources and improve productivity.

20

Remotely located individuals who are, for example, traveling on business, often need to access their organization's computer. A concern of many organizations is monitoring the costs of remote users accessing the host computer or computer network of the company, in addition to tracking the usage of computer time and various costs associated with that time.

25

Typically, each organization's computer facility tracks computer usage internally and generates various reports based on that information. Also, the costs associated with remotely dialing up an organization's computer facilities, such as the telephone line charges, are reported separately by each of the one or more long distance line carriers utilized

30

by the remotely located computer users. Additional costs of maintaining a remotely accessible computer network, such as supporting an information services person or department to handle difficulties with remote access by authorized users, may take up significant resources particularly in smaller organizations.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a preferred embodiment of a system for monitoring computer usage and costs associated with remote access according to the present invention.

FIG. 2 is a flow chart showing a preferred method of monitoring computer usage and costs using the system of FIG. 1.

DETAILED DESCRIPTION OF THE PRESENTLY PREFERRED EMBODIMENTS

An advantage of the present invention is consolidation of usage and billing information in a single report. Another advantage of the present invention is the ability to manipulate the usage and billing data for each of a number of different host computer networks by individual user and by predetermined groups or departments of users at each organization. The preferred method and system cooperate with a system for securing access between remotely located computer users and the computers of different organizations for which they are permitted access.

FIG. 1 illustrates a preferred system 10 for securing access between remotely located computer users and computers of different organizations in addition to monitoring access and maintaining billing records for each host computer system. The system 10 includes at least one remotely located user computer 12. A secure identification card 14 is associated with the user and the user computer 12. A user computer 12 preferably communicates over standard telephone lines, also known as plain old telephone service (POTS) lines 17, via modem 16 through the public switched telephone network (PSTN) 18. The system 10 of the present invention may use other commonly available communication devices, such as an ISDN terminal adapter or a communications server, in place of the analog modem. The user computer may be a personal computer or another computer network. One suitable secure ID card is available from Security Dynamics, Inc. of Cambridge, Massachusetts and

includes a display showing a time variant pass code for use by an authorized user in accessing a host computer network.

A communications server 20, which may be a router such as a Cisco 5200, is in communication with a security service bureau 22 over a frame relay network 18. The security service bureau 22 may be a local area network (LAN) 26 that includes at least one administrative workstation 28 for monitoring operation of the security service bureau.22. A suitable administrative workstation 28 may be any of a number of commonly available personal computers. A network access server (NAS) 30 is also connected to the LAN 26. The LAN 26 of the service bureau 22 connects to the frame relay network 24 via a firewall 32. The firewall may be a personal computer, such as those available from SUN Microsystems, running software available from SOLARIS to provide protection to the service bureau LAN 26 from outside corruption. The NAS 30 may be any of a number of servers available from Hewlett Packard, such as the HP712, HP755, or the HP720. The NAS 30 of the service bureau 22 controls access of remote users, through the communication server 20 and frame relay network 24, to the multiple host computer networks 34 or stand alone computers. In the example of FIG. 1, each of the host computer networks or stand alone computers utilize the service bureau to authenticate remote users at various computers 12. One system and method for authenticating users through a service bureau is disclosed in a commonly assigned, related application identified as Attorney Docket No. 8285/141. That application is filed on the same date as the present application and is hereby incorporated by reference in its entirety.

The system 10 also includes an integrated service center (ISC) 35 and an enterprise service system (ESS) 37. The ISC 35 preferably includes a computer configured to accept all service requests from various end user host computer networks desiring to add or remove computer use monitoring services or change the list of authorized users for the network. Additionally, the ISC 35 receives telephone calls from end users 12

seeking help relating to remote access services. The ISC 35 assigns help requests to the appropriate party in the system 10. In one embodiment, the ISC 35 is a vertically integrated service center and help desk for video, audio, and data communications.

5   The ESS 37 is a master database containing lists of periodic user charges, also known as "per seat" charges, for the various host computer systems serviced by the system 10. The ESS 37 also contains a list of field service fees associated with a respective host computer network 34 and records any extra services used by a host computer network 34 and

10   its authorized users. The fees for each particular host computer network are negotiated prior to beginning services to a particular host computer network and associated authorized users. The negotiated fees may be stored as tables in the ESS. The ESS 37 may be a server running UNIX software such as a SPARC Server available from SUN Microsystems.

15   The ESS receives updates on authorized users and subscribing host computer networks from the ISC.

A network management center (NMC) 39 is in communication with the ISC 35 and a private corporate intranet 19 via the ESS 37. The NMC 39 receives help requests from the ISC and provides a help desk for

20   network infrastructure problems, performance issues and chronic desktop problems. The NMC 39 uses a pre-entered user definition and information to create a trouble record for resolving issues associated with remote access services provided to the host computer networks 34. Each trouble call is stored at the NMC 39. The NMC serves to provide

25   proactive surveillance of all physical lines and communications servers in the system as well as handling trouble calls passed on from the ISC.

A customer service center (CSC) 40 is also linked to the system 10 via the ESS and the private corporate intranet 19. The CSC 40 manages the ordering of POTS services and repairs of business lines (e.g. DS1,

30   ISDN, etc.). A billing application communicates over the corporate intranet 19, via the ESS 37, with the NAS 30 and other system 10

components to obtain necessary billing information concerning host
computer networks 34 and their respective users. Preferably, the billing
application is a software application running within the ESS containing
logic necessary to organize cost data by per user and per entity within a

5   particular client's (host computers) organization. Alternatively, the billing
application may be a discrete billing computer 42 executing the necessary
logic to obtain and manipulate billing information.

Utilizing the system 10 described above, a preferred method of
monitoring access to each of the host computer networks subscribing to

10   the system security services is illustrated in FIG. 2. Each computer
network 34 provides an associated list of authorized users that is
maintained at the ISC, ESS, and NAS 30 (at step 50). An authorized user
accessing a host computer exchanges the information with the NAS 30,
via the communication server, each time the user dials in to gain access

15   to his respective host computer network 34. A starting time stamp is
created at the beginning of each remote access call received from a user
at the communication server 20 (at step 52). In a preferred embodiment,
the remote user accesses his respective host computer network by dialing
in through the PSTN 18 using a modem 16 or other communication device

20   to reach a network communications server 20. The communication
server 20 forwards information on the call through the frame relay network
24 to the service bureau 22. At the service bureau 22, the NAS 30
authenticates the user through the exchange of a user name and a pass
code.

25   The pass code preferably consists of a fixed personal identification
number and a time variable security token. The security token may be a
soft token, such as a software application on each authorized user's
computer, or a hard token, such as a secure ID card 14 available from
Security Dynamics, Inc. Each authorized user preferably has her own

30   security token and the security token may be a sequence of numbers,
letters, or other type of symbol. Using the secure ID card 14, the security

token is obtained by the user from a display that generates a new security token at predetermined time increments. The NAS 30, containing an identical security token generating algorithm synchronized with the secure ID card 14 generates the same security token to verify that the user is an

5   authorized user. On authentication, the communication server 20 connects the user computer 12 to the appropriate host computer 34 for the duration of the call. The NAS 30 receives an ending time stamp from the communication server 20 at the conclusion of the remote access call when the user hangs up or otherwise disconnects from the host computer

10   network 34 (at step 54). Following the conclusion of the remote access call, the service bureau stores the starting and ending time stamps in the NAS memory. Preferably the starting and ending time stamps are associated in the user log with the list of authorized users so that the user log contains a record of computer time usage for each authorized user (at

15   step 56).

After the end of the predetermined billing period, the user log is transmitted from the service bureau in a discrete file generated at the NAS to the billing computer 42 (at step 58). The billing period may be any desired length of time, such as a month or a year. The list of host

20   computer networks and associated list of authorized users for a host computer network is also transmitted to the billing computer (at step 60) from the NAS over the frame relay network. The billing computer then generates a billing summary for each of the subscribing customer host computer networks (at step 62).

25   As part of the process of developing a periodic bill for customers subscribing to the system, a long distance carrier invoice is electronically transmitted to the billing computer from a long distance telephone service provider. The long distance service provider may be any one of a number of available service providers, such as Ameritech, selected by the host

30   computer network. The long distance telephone service provider transmits a minutes of use invoice for the long distance access number

used by authorized users of a given host computer network to access the security service bureau. The long distance access number may be an "800" number or other telephone number dedicated for use by authorized users to communicate with the appropriate host computer through the

5   system 10.

Because each authorized user of a given host computer network is provided with the same telephone number, the billing computer can use the unique pass code each user possesses to distribute the minutes of use charge to the appropriate user. Preferably, the long distance charges

10   are distributed appropriately among the users of each host computer network based on a user's percentage of computer access time for that billing period. The ESS 39 provides fixed expense information to the billing computer 42 by way of monthly per seat charges and incident charges. Incident charges refer to the fees assessed to calls by

15   authorized users to the system help desk at the CSC.

Using all the information gathered, the billing computer based on the subscribed for services and the usage of each individual authorized user, various usage information and billing forms will be created. For example, in one preferred embodiment a bill may be generated that

20   breaks up authorized users into the various departments to which they are assigned within a customer's organization. For each authorized user in the department a predetermined group of information may be displayed. This information may include per seat charges, the cost of long distance telephone usage (distributed among authorized users based on the

25   amount of time a user was communicating with the host computer network), any equipment charges, maintenance charges, and miscellaneous charges. The per seat charges refer to fixed service charges associated with supporting each authorized user. The miscellaneous costs may include incidental security cost such as

30   replacing secure ID cards, or for particular pieces of software necessary for enabling remote users to access their host network through the

security service bureau 22. Optionally included in the per seat charges are the local exchange and other incidental charges. Once the billing summary has been generated, the billing computer can transmit the billing summary directly to the appropriate host computer network. The

5   transmission may be done via e-mail over an internet connection, via facsimile, or through other means.

Another aspect of the presently preferred invention is that computer usage information may be provided to the customer and the service provider maintaining the security service bureau 22 so that computer

10   resources may be optimized for usage patterns. For example, the billing computer may generate monthly or annual reports dividing up the usage for each individual authorized user by total time used per a given period or by time of day or week so that host computer network 34 or service bureau 22 resources can be properly allocated for particularly heavy

15   usage.

From the above, a new system and method of monitoring access and fees for host computer networks with relocated users is provided. The method includes maintaining a list of host computer networks and associated list of authorized users for each network, creating a starting

20   and ending time stamp for remote access calls, transmitting the starting and ending time stamps in the user log to a billing computer in addition to other billing information, and generating a billing summary of costs and usage at the billing computer. The system preferably includes a security service bureau providing secure remote access between remotely located

25   authorized users and their respective proprietary host networks. In one preferred embodiment, the NAS preferably records time stamps and a user log indicating usage of resources by individual authorized users. A billing computer is also included in the system having the logic necessary to compile information from the user log in the security service bureau and

30   cost information received from outside sources to generate a periodic bill indicating cost per individual user and/or department.

It is intended that the foregoing detailed description be regarded as illustrative rather than limiting, and that it be understood that the following claims, including all equivalents, are intended to define the scope of this invention.

WE CLAIM:

1.   In a system for providing secure remote access between a plurality of host computer networks and a plurality of authorized users via

5   a network access server, a method of monitoring access to each of the host computer networks comprising the steps of:

maintaining a list of host computer networks and an associated list of authorized users for each host computer network in a first memory device;

10   creating a starting time stamp at the beginning of a remote access call received from an authorized user at the communication server;

creating an ending time stamp at a conclusion of the remote access call;

storing the starting and ending time stamps for the remote

15   access call in a user log in the network access server, the starting and ending time stamps associated with the list of authorized users whereby the user log contains a record of computer time usage for each authorized user;

transmitting the user log from the network access server to a

20   billing computer;

transmitting the list of host computer networks and the associated list of authorized users for each host computer network from the first memory device to the billing computer; and

generating a billing summary at the billing computer for each

25   of the host computer networks.

2.   The method of claim 1, wherein the list of host computer networks further comprises a fee schedule associated with each of the host computer networks, the fee schedule being a predetermined list of

30   standard charges and the step of generating a billing summary comprises comparing the user log to the fee schedule for each respective host

computer network and determining a total fee for each of the host computer networks.

      3.   The method of claim 1, wherein the system further
5   comprises a help desk computer and the method further comprises:
          storing a list of telephone calls received at the help desk
computer from authorized users, each telephone call in the list of
telephone calls associated with an authorized user; and
          transmitting the list of telephone calls to the billing computer.
10

      4.   The method of claim 3, wherein the step of generating a
billing summary further comprises generating a list of usage charges and
generating a list of help desk charges for each host computer network
from the user log and the list of telephone calls.
15

      5.   The method of claim 4, wherein the step of generating a
billing summary comprises generating a billing summary for each
authorized user of each host computer network, the billing summary
having a list of authorized users for the respective host computer network,
20   an associated usage charge for each of the authorized users, and an
associated list of telephone calls for each associated user.

      6.   The method of claim 1, further comprising:
          receiving a long distance telephone company report of total
25   time usage of a network access telephone number and the billing
computer; and
          determining a per user cost ratio for each of the authorized
users of the host computer network using the network access telephone
number from the long distance telephone company report and the user
30   log.

7.   The method of claim 1, wherein the list of host computer networks comprises a list of company departments, each company department associated with a predetermined number of authorized users and the step of generating a billing summary comprises calculating a total usage for each company department from the user log and the list of company departments.

8.   The method of claim 7, wherein the list of host computer networks further comprises a fee schedule associated with each of the host computer networks, the fee schedule being a predetermined list of standard charges and the step of generating a billing summary comprises calculating a fee for each company department based on the fee schedule and the calculated total usage for each company department.

9.   The method of claim 1 further comprising the step of transmitting each billing summary for each host computer network from the billing computer to the host computer networks, each billing summary directed to a respective one of the plurality of host computer networks.

10.   The method of claim 9, wherein the step of transmitting each billing summary comprises sending the billing summary via e-mail.

11.   The method of claim 9 wherein the step of transmitting each billing summary comprises sending each billing summary via facsimile from the billing computer.

12.   A system for generating billing and usage information for each of a plurality of host computer networks utilizing security services from a remotely located security server, the system comprising:

a first memory device containing a list of authorized users for each of the plurality of host computer networks;

a second memory device containing means for generating and storing a user log, the user log having a list of remote access call start times and a list of remote access call end times; and

a billing computer in communication with the first and
5   second memory devices, the billing computer for receiving information from the first and second memory devices and generating a bill.

13.   The system of claim 12, further comprising a help desk computer in communication with the billing computer, the help desk
10   computer having a memory containing a list of authorized users who have accessed the help desk over a predetermined time period.

14.   The system of claim 12, wherein the first memory device further comprises a fee schedule for each of the plurality of host computer
15   networks.

15.   The system of claim 14, wherein the first memory device further comprises a list of groups for each host computer network, wherein the authorized users for each host computer are associated with a group
20   in the list of groups.
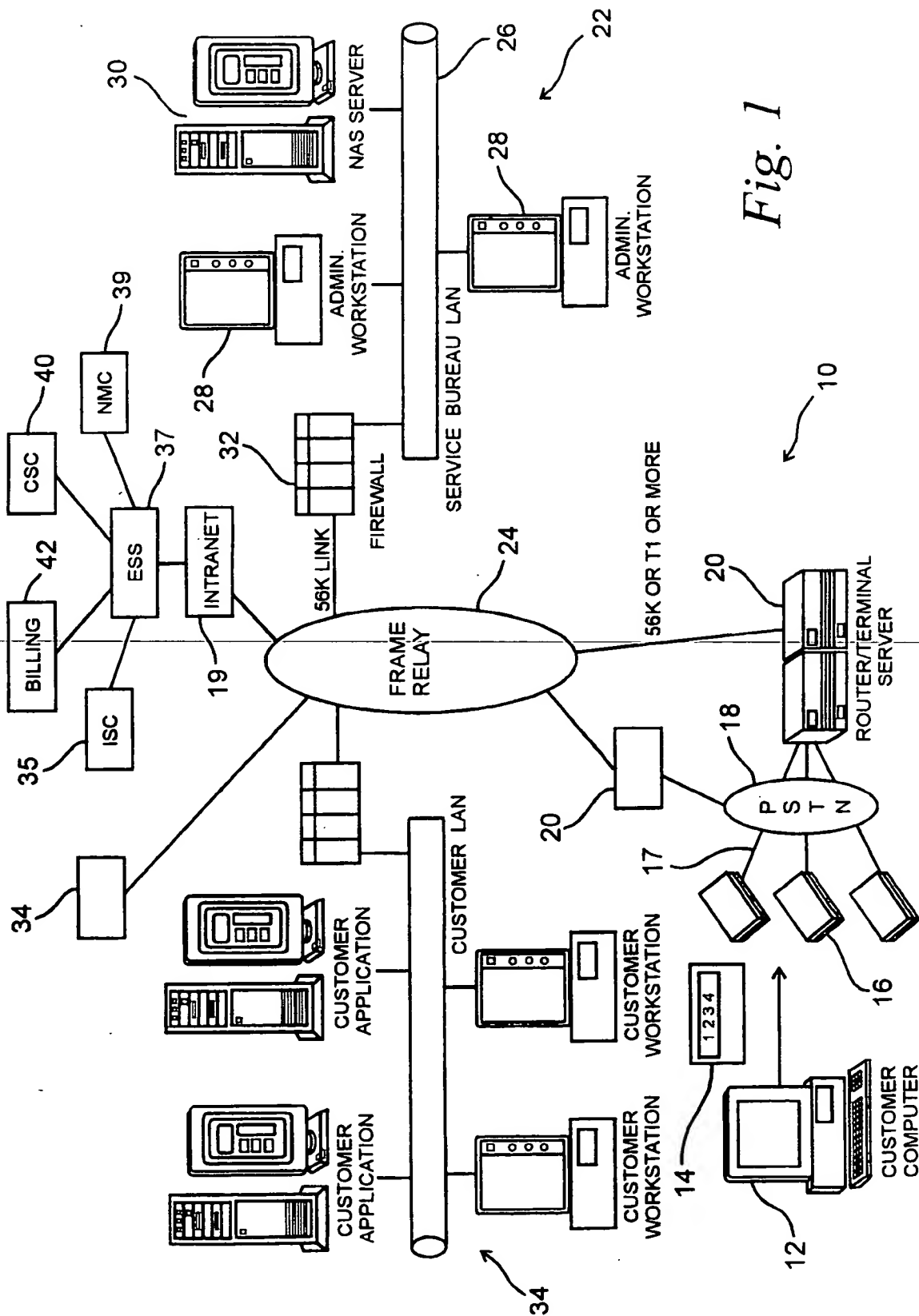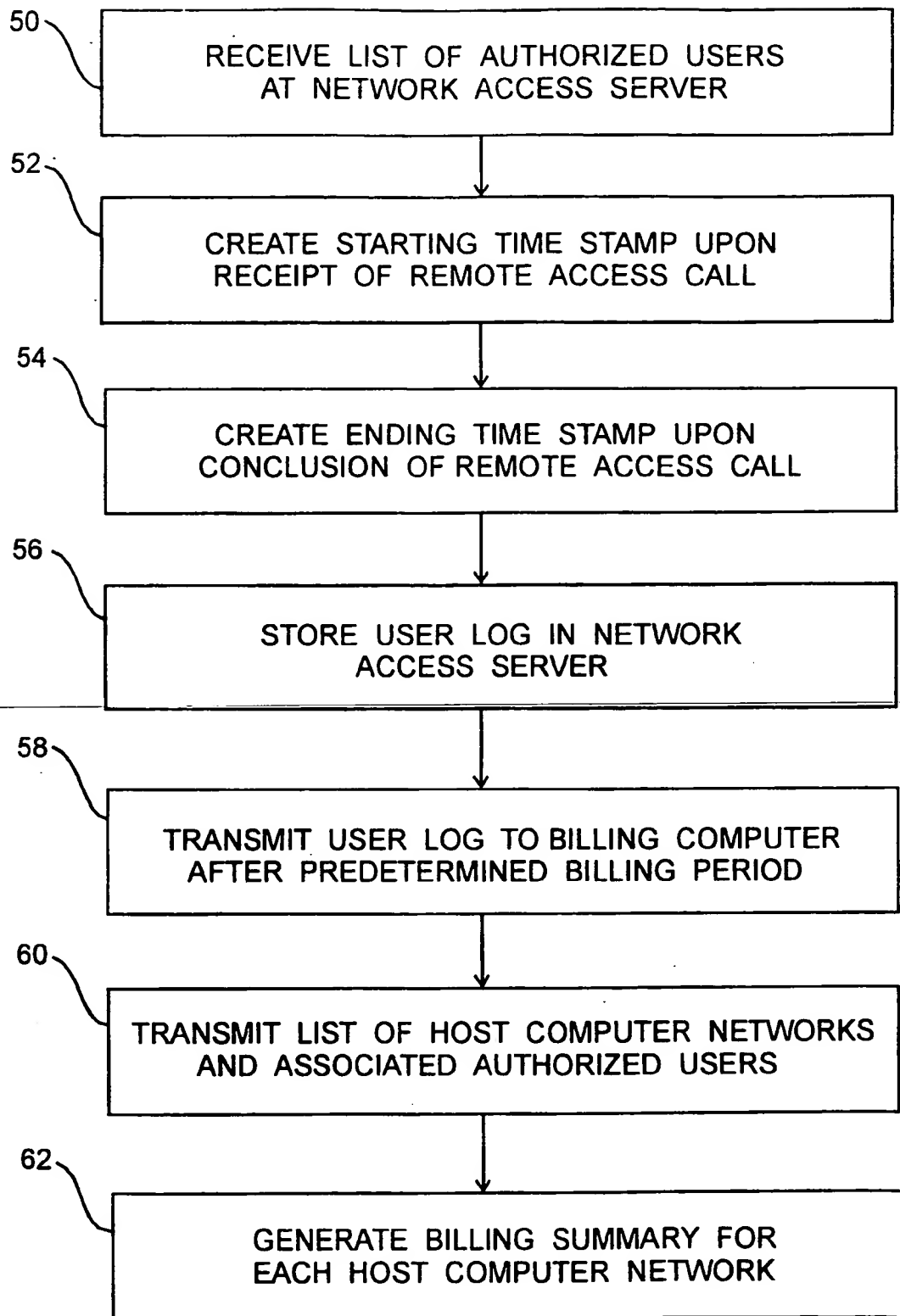
Fig. 1

```
50 ┌─────────────────────────────────────────┐
   │      RECEIVE LIST OF AUTHORIZED USERS     │
   │         AT NETWORK ACCESS SERVER          │
   └─────────────────────────────────────────┘
                        │
                        ▼
52 ┌─────────────────────────────────────────┐
   │      CREATE STARTING TIME STAMP UPON      │
   │      RECEIPT OF REMOTE ACCESS CALL        │
   └─────────────────────────────────────────┘
                        │
                        ▼
54 ┌─────────────────────────────────────────┐
   │       CREATE ENDING TIME STAMP UPON       │
   │      CONCLUSION OF REMOTE ACCESS CALL     │
   └─────────────────────────────────────────┘
                        │
                        ▼
56 ┌─────────────────────────────────────────┐
   │       STORE USER LOG IN NETWORK           │
   │             ACCESS SERVER                 │
   └─────────────────────────────────────────┘
                        │
                        ▼
58 ┌─────────────────────────────────────────┐
   │   TRANSMIT USER LOG TO BILLING COMPUTER   │
   │   AFTER PREDETERMINED BILLING PERIOD      │
   └─────────────────────────────────────────┘
                        │
                        ▼
60 ┌─────────────────────────────────────────┐
   │  TRANSMIT LIST OF HOST COMPUTER NETWORKS  │
   │    AND ASSOCIATED AUTHORIZED USERS        │
   └─────────────────────────────────────────┘
                        │
                        ▼
62 ┌─────────────────────────────────────────┐
   │      GENERATE BILLING SUMMARY FOR         │
   │      EACH HOST COMPUTER NETWORK           │
   └─────────────────────────────────────────┘
```

Fig. 2

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER	

IPC(6)   :G06F 17/60; H04N 1/00
US CL   :705/32; 395/324; 358/402
According to International Patent Classification (IPC) or to both national classification and IPC

B.   FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

  U.S. : 705/32; 395/324; 358/402; 705/34

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

  APS
computer network, starting time, ending time, billing computer, fee schedule, long distance.

C.   DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,493,492 A (CRAMER et al) 20 February 1996, abstract, figures 2, 3; col. 1; col. 2, lines 1-10; col. 3, lines 9-23.	1, 12
Y	US 5,696,906 A (PETERS et al) 09 December 1997, figure 4, col. 2, lines 15-45; col. 3, lines 45-65; col. 4, lines 40-67; col. 5; col. 6.	2-6, 7-8, 9-11, 13-15
Y	US 5,508,817 A (KUNIGAMI) 16 April 1996, figure 5, col. 6, lines 15-40.	2-5, 7-8, 9-11, 13-15
Y,P	US 5,802,502 A (GELL et al) 01 September 1998, col. 1, lines 24-33.	6

☐   Further documents are listed in the continuation of Box C.   ☐   See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search 11 MARCH 1999	Date of mailing of the international search report **14 APR 1999**
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JAMES P. TRAMMELL Telephone No. (703) 305-9768

Form PCT/ISA/210 (second sheet)(July 1992) ★